UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/876,568	06/07/2001	Jalaludeen Ca	Ca 3-2	7799

47386 7590 01/30/2007

RYAN, MASON & LEWIS, LLP
1300 POST ROAD
SUITE 205
FAIRFIELD, CT 06824

EXAMINER
POLTORAK, PIOTR

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
01/30/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

MAILED

JAN 30 2007

Technology Center 2100

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR / PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
09/876,568			

EXAMINER

ART UNIT	PAPER
	20061106

DATE MAILED:

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

In response to the Order Returning Undocketed Appeal to the examiner from BPAI, herein is attached the requested information: a listing of evidence relied on including relevant pages of patent and non-patent references.

KAMBIZ ZAND
PRIMARY EXAMINER

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/876,568
Filing Date: June 07, 2001
Appellant(s): CA ET AL.

Kevin M. Mason
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 2/16/06 appealing from the Office action mailed 08/09/05.

(1) Real Party in Interest

A statement identifying by name the real party in interest as AGERE SYSTEMS GUARDIAN CORP is contained in the brief.

(2) Related Appeals and Interferences

The brief indicated no related appeals and interferences, which directly affect or be directly affected by or have a bearing on the decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

- Cromer et al. (U.S. Patent No. 6021493), *hereinafter Cromer*,
- Sanders et al. (U.S. Patent No. 5231375), *hereinafter Sanders,*
- Lam (U.S. Patent No. 6140923),

- Pearce (U.S. Patent No.6308272),
- Minasi (Mark Minasi, "Mastering Windows NT Server 4, 6th edition, 1999, ISBN: 0782124453), pg. 378, 380 and 434,
- Thurrott (Paul Thurrott, "What's new in Windows 2000 RC2 Reviewed", http://www.winsupersite.com/reviews/win2k_rc2_whatsnew.asp), pg. 1-3,
- Computer Dictionary ("Charles J. Sippl and Roger J. Sippl "Computer Dictionary and handbook", 3rd edition, 1980, ISBN: 0-672-21632-9),
- Sobell (Mark G. Sobell, "A practical guide to the UNIX system, 3rd Edition, 1997, ISBN: 0805375651).

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

Claims 1,10, 17, 22, 26-29 and 31-32 are rejected under 35 U.S.C. 102(b) as being anticipated by Thurrott (Paul Thurrott, "What's new in Windows 2000 RC2 Reviewed", http://www.winsupersite.com/reviews/win2k_rc2_whatsnew.asp).

Thurrott teaches monitoring a network connection and generating an alarm if the network connection is disconnected (Network disconnect cue section).

Windows 2000 RC2 taught by Thurrott is implemented on computers comprising memory and processors and codes.

Claim Rejections - 35 USC § 102 or 103

Claims 1, 7-10, 12, 17, 22, 26-29 and 31-32 are rejected under 35 U.S.C. 102 as being anticipated by or, in the alternative, under 103(a) as obvious over Cromer et al. (U.S. Patent No. 6021493).

As per claims 1, 7-9, 26-28 Cromer et al. teach a system and method for detecting when a computer system is removed from a network (col. 2 lines 17-19). In particular Cromer et al. teach LAN software application running on the remote computer system or server that has a list of LAN clients addresses. The software polls client computers and if it does not get a response back after a predetermined number of retries, it generates an alarm resulting in alerting a LAN administrator that a client is now not attached to the LAN (col. 7 lines 31-49). This reads on: "detecting removal of a device connected to a network by a network connection comprising monitoring the network connection and generating an alarm if the network connection is disconnected.

Cromer et al. does not explicitly teach that an alarm is generated in the removed device. However, disconnecting the remote computer system (or server) would result in lack of response to sent polls by the software application hosted on the computer system. As a result the alarm would have been generated on the device disconnected from the network. Even if disconnection of the remote computer system did not result in generation of the alarm it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to implement such a modification. One of ordinary skill in the art would have been

motivated to perform such a modification in order to warn about a computer (in this case the remote computer system) being removed from a network.

Claims 17, 22 and 31-32 are substantially equivalent to claim 1; therefore claims 17, 22 and 31-32 are similarly rejected.

As per claim 12 Cromer et al. teach waiting for a response for a predefined time interval (col. 8 lines 35-40).

As per claims 10 and 29 Cromer et al. teach LAN communication utilizing IP addresses (col. 8 line 47).

Claim Rejections - 35 USC § 103

Claims 2-3, 13-14, 18-19 and 23-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cromer et al. (U.S. Patent No. 6021493) in view of Sanders et al. (U.S. Patent No. 5231375) and in further view of Lam (U.S. Patent No. 6140923).

Cromer et al. teach generating an alarm if a network connection is disconnected.

As per claims 2, 13, 18, 23 Cromer et al. do not teach that the generated alarm generates an audio output and do not teach preventing a volume of an audio output of the device from being reduced below a predefined minimum level.

Sanders et al. teach a device (Sanders et al., theft detection and alarm system, Sanders et al., Fig. 1 object 1010) connected to a network (Interface Unit 1020, Data transmission System 1030, Interface Unit 1040, Theft and alarm system monitor 1050 and database1060, Fig. 1) by a network connection, that produces an audible alarm signal in the device (that prevents a volume of an audio output of the device from being reduced below a predefined minimum level) when a

network connection is disconnected (Sanders et al., Fig. 2, col. 5 lines 33-38), and Lam provides a motivation to combine (Lam, col. 48-51).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to generate an alarm in the removed device as taught by Sanders et al. One of ordinary skill in the art would have been motivated to perform such a modification in order to draw attention to the device.

Preventing a volume of an audio output of the device from being reduced below a predefined minimum level (as implemented in Sanders et al.'s invention) is implicit, since lowering the volume could prevent drawing attention to the device.

As per claims 3, 14, 19 and 24 the device implementing audible alarm system taught by Sanders et al. prevents the device from being turned off (Sanders et al., Fig. 6 and col. 11 lines 46-49). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to extend *Cromer's* invention by preventing the device from being turned off given the benefit of efficient network administration e.g. monitoring the network devices while preventing terminating the monitoring invented by *Cromer* that would occur if the device was turned off.

Claims 3, 14, 19 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cromer et al. (U.S. Patent No. 6021493) in view of Minasi (Mark Minasi, "Mastering Windows NT Server 4, 6th edition, 1999, ISBN: 0782124453)

Cromer teaches a system and method for detecting when a computer system is removed from a network. Cromer does not teach preventing the turning off a device.

Minasi teaches assigning rights to users that grant or deny access to certain objects (resources) such as turning off a device (Minasi, pg. 378 §3 and, shut down rights pg. 380, turning off a device in particular). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to implement Minasi's teaching preventing the turning off a device in order to prevent said devices from being turned off mistakenly and thereby causing false alarms.

Claims 4-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cromer et al. (U.S. Patent No. 6021493) in view of Pearce (U.S. Patent No.6308272).

Cromer et al. teach monitoring a network connection as discussed above. Cromer et al. do not explicitly address how said monitoring step is activated. As per claim 4 Pearce teaches monitoring that is set to activate automatically in a passive manner (provide security during a selected period of time, col. 6 lines 61-68). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to configure monitoring being activated automatically in a passive manner as taught by Pearce in order to activate monitoring at times where the threat of a network problem is most likely to occur (e.g. after work hours) and in order to avoid false alarms (avoid hours of scheduled network maintenance, re-configuration etc.). Also, it is implicit that the period time is selected by the user who must manually configure and activate the system in order for monitoring to be automatically activated in a passive manner, thus reading on claim 5.

Claims 6, 11, 15-16, 20-21, 25 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cromer et al. (U.S. Patent No. 6021493) in view of Sobell (Mark G. Sobell, "A practical guide to the UNIX system, 3rd Edition, 1997, ISBN: 0805375651).

Cromer et al. teach monitoring a network connection as discussed above.

Cromer et al. do not teach a generating step being prevented by entering a password.

Sobell teaches using a password to perform administrative tasks (login as the Superuser, pg. 493).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use password as taught by Sobell in order to perform administrative tasks limited only to authorized (administrative and supportive) staff. One of ordinary skill in the art would have been motivated to perform such a modification in order to be able to perform administrative tasks such as device relocations, troubleshooting, network upgrade etc. without triggering false alarms.

(10) Response to Argument

On page 4 appellant contests independent claims 1, 17, 22 and 31 as rejected under Thurrott.

Appellant argues that Thurrot's visual cue alerts are unlikely to be effective as an alarm to alert one or more individuals to a theft, as would be apparent to a person of ordinary skill in the art. Appellant concludes by stating that "a person of ordinary skill in the art

would not interpret the visual cue disclosed by Thurrott as an alarm for indicating a theft".

The examiner points out that *Thurrott* clearly discloses the alarm as cited in the claim language.

Computer Dictionary provides the definition of an "alarm" to be "a signal, by display or audio device, which signifies that an error has occurred, or an emergency condition exists that is interfering or could interfere with the proper execution or completion of a program" *(Computer Dictionary, pg. 12)*. This definition is consistent with common interpretation in the art see *Shimizu et al., U.S. Patent No. 5689416, col. 4 lines 17-18, 33-40; Low, U.S. Pub. No. 2003/0101251, [109], [120] and Fig. 33 or Kimura, U.S. Patent No. 5372436, col. 15 lines 5-6* for example.

Thurrott's icon alarming a user that a network cable became unplugged *(Network disconnect cue section and Fig. 3)* unambiguously reads on generating an alarm since unplugging the cable results in a condition that can and does interfere with the proper execution or completion of at least programs requiring a network connection *(e.g. back up of critical files to a remote computer)* and alarming the user about the condition. Disconnecting a cable providing a network connection to a device removes the device from the network, regardless of how critical it is to maintain a connection between the device and other network devices still connected to the network.

In regard to appellant's argument that *Thurrott's* reference does not explicitly address "indication of a theft" the examiner points out that "indication of theft" is not present in any of the claims 1, 17, 22 and 31. Claims 1, 17, 22 and 31 recite only in the preambles "removal of a device connected to a network".

Summarizing, *Thurrott* clearly teaches monitoring network connection of a device and generating an alarm in the (removed) device if the network connection is disconnected.

On page 4-5 appellant contests independent claims 1, 17, 22 and 31 rejected under Cromer.

Appellant argues that Cromer does not disclose or suggest generating an alarm in the removed device. Appellant then presumes that Cromer teaches away from the present invention by teaching to install an alarm outside of the protected device.

Before addressing appellants' arguments the examiner points out that in *Cromer's* invention **the remote computer system or server 34** as well as **the software application** (Cromer, col. 7 line 35) **read on "a device"** recited in the claim limitations. Computers *(clients, servers, remote computers, network nodes etc.)* perform particular functions thanks to software that is implemented on the computers. As a result, in regard to the current application, a method implemented by software cited by *Cromer* should not be considered as a method implemented by some separate network entity

but rather as a method implemented by a device (the remote computer system or server) on which the software is executed.

For example, as cited by appellant regarding *Cromer's* col. 7, lines 41-49 the functions performed by software application are actually actions performed by a remote computer or server 34 *(hereinafter a device)* that runs the software *(col. 7 lines 34-35).*

Thus, reading *Cromer's* citation the remote computer system or server 34 as well as software application should be considered as matching the term "the device" used in the claim language and the term should be considered distinct from "a client" recited by *Cromer.*

The term "client" recited by *Cromer* corresponds to a second device *(claim 12)* and/or a remote device *(claim 17).*

The claim language calls for monitoring a network connection of a device and generating an alarm in the *(removed)* device if the network connection is disconnected.

Network consists of all of the computer's residing on the same network. Thus, both: clients and the device *(a remote computer or a server 34)* cited by Cromer reside on the same network should be considered as "devices connected to the network".

As a result generating an alarm in a device *(taught by Cromer)* that is a result of removing the device from the network reads on "generating an alarm in the removed device".

As per *Cromer's* teaching:

> *"when the client receives this packet it transmits a packet back to the LAN indicating it is still on the LAN. If the software application gets a response back then it just moves to the next client. If the software application does not get a response back after a predetermined number of retries, it indicates to the LAN administrator though a message that the client at this location is now not attached to the LAN and can be assumed missing or stolen" (Col. 7, lines 41-49)*

Appellant argues (pg. 5) that *Cromer* discloses that the software application that receives the response from the client (and not the client) is the application that sends a message to the LAN administrator. Appellant concludes the arguments with an assertion that *Cromer* does not teach "generating an alarm in the removed device" if the network connection is disconnected.

The examiner points out that although the software application indeed receives responses from the client, appellant's assertion that *Cromer* does not teach "generating an alarm in the removed device" is incorrect.

As previously discussed the application software is not an independent entity but it is an entity utilized by a device *(the remote computer system or server, Cromer col. 7 lines 34-35).* With this in mind, the examiner would like to point out the facts regarding events that take place in *Cromer's* invention.

As clearly disclosed by *Cromer* and cited by appellant *("...if the software application does not get a response back after a predetermined number of retries...")* the device *(utilizing the software application)* sends network enquiries *(polls a network client)* and based on the outcome *(response or no response)* it determines a status of the network connection *(connection between the device and the network)*. As a result, the response coming from the network client signifies the fact that there is a network connection.
In other words, the device in *Cromer's* invention verifies a status of network connection and if no network connection *(no response)* is detected an alarm is generated.

The examiner also emphasizes that not only clients but also the device is connected to the network. As a result disconnecting a network connection removes the device from the network, and consequently prevents the device from receiving the responses.

The reason is very simple: the requests directed to network clients will never reach the network and thus it will not reach the clients either. Even if the requests were sent prior to disconnecting the network connection, as soon as the device is removed from the network any returning responses from clients will fail to reach the device.
The lack of responses results in the device generating an alarm.

Cromer clearly teaches generating an alarm on the device *(Cromer, col. 9 lines 21-23)*. The alert generated and sent out by the device reads on the alarm since it is a signal

indicative of an emergency condition. Note that the "client is missing" recited in *Cromer* in col. 9 lines 21-23 is based on no response from the client *(col. 7 lines 44-48).* Also, one should not focus on the fact that due to the problem with the network connection the generated alarm may not reach the intended destination but rather the focus should be on the fact that the alarm signal is generated if the device (or a client) is removed from the network.

As per "monitoring a network connection", as previously shown, removing the network connection results in generating an alarm. Of course, discovering that the network connection is removed can only be possible in the case where the network connection is monitored. In *Cromer's* invention such a monitoring is achieved by polling *(that is sending a response and receiving a response, Cromer, col. 7 lines 32-49)* network clients.

Summarizing, *Cromer* clearly teaches a method for detecting removal of a device connected to a network by a network connection *(a remote computer or a server 34 using software application polls a network, Cromer, col. 7 lines 31-49 and col. 9 lines 19-23)*, comprising monitoring network connection of a device *(is the device connected or not connected to the network; that is does the device receive responses from the network, e.g. from a network client, Cromer, col. 7 lines 40-46)* and generating an alarm *(generate an alarm notifying about the disconnected network*

connection) in the removed device if the network connection is disconnected *(Cromer, col. 9 lines 21-23).*

On page 5 appellant contests the rejection of independent claims 1, 17, 22 and 31. *In particular appellant argues that Cromer and Thurrott alone or in combination do not disclose or suggest generating an alarm in the removed device if the response is no longer received or not received within a predefined time interval.*

As per the received response that is no longer received, Cromer clearly indicates that when the removed device *(implementing the software)* does not receive a response from the network the device is aware that there is no present network connection and this is what triggers the alarm on the removed device *(col. 7 lines 44-48).* Of course, removing the network device from the network *(disconnecting the network connection)* will result in no longer receiving any responses from the network.

As per a predefined time interval, *Cromer* discloses a predetermined time that each request for the response is sent *(col. 7 lines 37-40)* and that the device waits for the response and only after it "does not get a response back after a predetermined number of retries" it assumes the network connection has been disconnected *(Cromer, col. 7 lines 44-48).*

On page 6 appellant continues to contest the rejection of independent claims 1, 17, 22 and 31.

On page 6-8 appellant discusses Sanders et al., Lam, Minasi, Pearce and Sobell with respect to claims 1, 17, 22 and 31.

Since neither of the cited references was used against the independent claims 1, 17, 22 and 31 the examiner does not traverse applicant's arguments.

On page 8-9 appellant contests the rejection of dependent claims 2, 13, 18 and 23 rejected under Cromer in view of Sanders and Lam.

Appellant argues that Thurrott, Cromer, Sanders, Lam, Minasi, Pearce and Sobell, alone or in any combination do not disclose or suggest preventing a volume of an audio output of the device from being reduced below a predefined minimum level.

Appellant also specifically cites Sander's col. 5 lines 33-38 as evidence of not teaching preventing a volume of an audio output of the device from being reduced below a predefined minimum volume.

Cromer's invention has been discussed above.

Since *Cromer* did not disclose an alarm in audible form *(an audio output of the device)* the examiner introduced *Sanders* that extends *Cromer's* invention with an audio output of the device that is utilized for an audible alarm signal in the device *(Sanders, col. 5*

lines 33-38). Furthermore, the examiner disclosed *Lam's* invention that provides motivation to combine *Cromer's and Sander's* inventions.

In particular, *Lam* stresses an importance of an audible alarm signal *(Lam, col. 2 lines 27-29 and col. 1 lines 52-58).*

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to extend *Cromer's* invention with an audio output sounding an audible alarm signal given the benefit of strong notification of occurrence of the alarm condition.

Cromer in view of *Sander* and *Lam* do not explicitly recite preventing a volume of an audio output of the device from being reduced below a predefined minimum level. However, preventing a volume of an audio output of the device from being reduced below a predefined minimum level would have been obvious to one of ordinary skill in the art at the time of applicant's invention given the fact that lowering the volume of the alarm could defeat the purpose of the audible alarm, especially since an unauthorized person *(e.g. a thief)* would have a particular interest in disabling the audible alarm.

In addition, the examiner once again points to *Sander's* alarm system that produces an audible alarm. As clearly disclosed in col. 11 lines 49-55 *Sander* is particularly concerned with affecting an alarm *(including volume)* and takes special precaution to prevent silencing *(that would also read on lowering the volume)* the alarm system.

Summarizing, *Cromer* in view of *Sander* and *Lam* teach an audio output of the device strongly notifying about an emergency condition. Furthermore preventing reduction of a volume below a predefined minimum level would have been obvious to one of ordinary skill in the art at the time of applicant's invention given the fact that reducing the volume could defeat the purpose of the audio alarm implementation.

On page 9-10 appellant contests rejection of dependent claims 3, 14, 19 and 24. *Appellant argues that the Cromer, Sanders, Lam and Minasi do not disclose or suggest preventing the device from being turned off.*

Cromer's invention has been discussed above.

Since *Cromer* did not explicitly teach preventing the device from being turned off, the examiner introduced *Minasi* who stresses the importance of effective administration of networks with a plurality of computers *(Minasi, "System Policies: Central Registry Control", pg. 434)*. The discussion of the administration is continued on pg. 378 where *Minasi* discusses user rights *(Minasi, "User Rights and Object Permissions")*. On pg. 380 *Minasi* concludes by providing variables that could be administrated. One of these variables is "Shut down the system" that can be granted to users.

The examiner points out that the existence of "shutting down the system" variable means that just as "shutting down the system" can be granted, the "shutting down the

system" privilege can be revoked. As a result, *Minasi* inherently teaches "preventing shutting down the system".

Cromer's invention aims towards theft protection as well as network monitoring *(Cromer, col. 7 lines 31-49)*. Turning the device off (shut down the device) would defeat the purpose of *Cromer's* invention.

As a result, extending *Cromer's* invention with preventing the device from being turned off would have been obvious to one of ordinary skill in the art at the time of applicant's invention. One of ordinary skill in the art would have been motivated to perform such a modification given the benefit of efficient network administration e.g. monitoring the network devices while preventing terminating the monitoring invented by *Cromer* that would occur if the device was turned off.

In addition, the examiner once again points to *Sander's* alarm system that produces an audible alarm. As clearly disclosed in col. 11 lines 49-55 *Sander* is particularly concerned with the possibility of turning off the alarm system. Not only does the alarm system device *(Fig. 2-3, object 1010)* have no output allowing the device to be turned off, but *Sander* also explicitly discloses an internal battery power that prevents turning off the device by removal of a power cord *(col. 11 lines 49-55)*.

Thus, extending *Cromer's* invention with preventing the device from being turned off would have been obvious to one of ordinary skill in the art at the time of applicant's invention. One of ordinary skill in the art would have been motivated to perform such a

modification given the benefit of efficient network administration e.g. monitoring the network devices while preventing terminating the monitoring invented by *Cromer* that would occur if the device was turned off.

Summarizing, *Cromer* in view of *Minasi* teach preventing the device from being turned off given the benefit of efficient network administration that includes monitoring the network devices while preventing termination of the monitoring invented by *Cromer* that would occur if the device was turned off.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Peter Poltorak

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Conferees:

Kim Vu,

Justin Darrow.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the

Related Appeals and Interferences section of this examiner's answer.